

# Overseeing Your Infrastructure

## Global Scan

The **Global Scan** dashboard enables you to view the current status of all of the Elements (servers and devices, Applications, and SLAs) in your environment. When initially viewed, the **Global Scan** dashboard is displayed, and typically contains a list of all the Elements that are being monitored by up.time .The **Elements** table displays the following information:

- the status and number of services that are associated with the Element
- the number of recent service outages
- CPU usage
- hard disk usage
- memory usage

For convenience, you can sort the **Elements** table by any outage type.

Service status indicators range from normal (green), to Warning (yellow), to Critical (red), and also include an Unknown state (gray). An Unknown state indicates that no performance data for the last 10 minutes exists for the Element. To avoid false positives, note that recently added Elements will have this status until 10 minutes' worth of performance data has been collected; also, in cases where the up.time Data Collector service is down for more than 10 minutes, all Elements will have this status until the service has been restarted and enough data has been collected.

The thresholds for the service status indicators are typically 70% for a warning state, and 90% for a critical state. These thresholds can be customized (see [Changing Reporting Thresholds](#)).

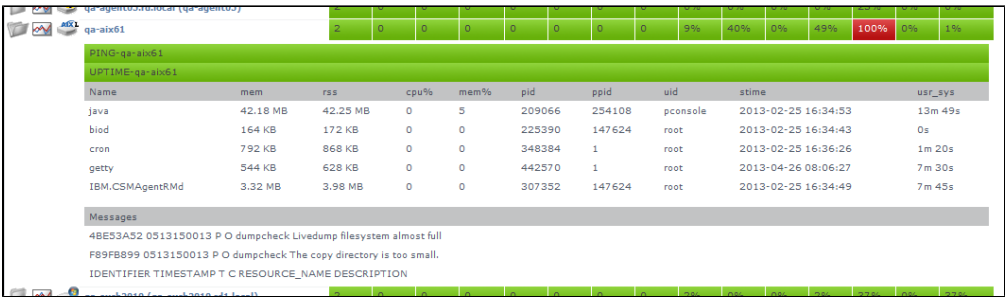
The **Recent Incidents** bar chart at the top left displays, in real-time, the number of service monitors that reported a non-OK status (CRIT, WARN, UNKNOWN, MAINT) during each of the past 24 hours. Note that host rechecks are included in the incident tally.

The **Current Service Status** pie chart at the top right visualizes the current availability of systems or devices. The services for unmonitored systems in groups are not shown in the pie chart.

## Viewing More Information

You can view detailed information about an Element by clicking its name. To view the details of each metric (for example, CPU usage) click the number in the column for that variable to go to its Graphing page, where you will be able to generate a graph.

When you click the file folder icon to the left of a system name, an expanded view of the server information appears:



up.time displays the following information for the system in the expanded view:

- the first section displays the names of the services associated with the Element, as well as their current states
- the second section lists the top five CPU-consuming processes for the Element
- the third section displays up to five of the most recent error messages reported by the up.time agent or Windows' Service Control Manager

## Groups and Views in the Global Scan Dashboard

When you create groups or views (see [Working with Groups](#) and [Working with Views](#)), they appear in their own sections in the **Global Scan** dashboard. The following information is displayed:

- the names and descriptions of the groups
- the number of Elements in each group
- the status of the hosts that make up the group
- the number of alerts per group

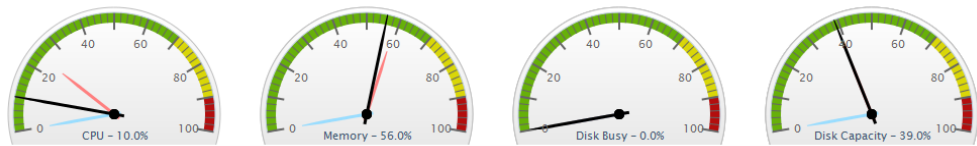
When you click a group or view in the **Global Scan** dashboard, the systems that make up the group or view and details about their status are displayed.

## Resource Scan

Resource Scan is a dynamically-updated dashboard that reports the percentage of various resources that are being used by the servers and groups of servers in your environment. Access this dashboard by clicking the **Resource Scan** tab. This dashboard is comprised of several components: performance gauges, charts, and Element tables.

## Performance Gauges

The row of gauges is updated every 15 minutes based on the most recently collected data:



The dials display averages of the most recent 15-minute time interval, as well as the maximum and minimum values recorded over the past 24 hours up to the most recent time frame. The gauges show the following information:

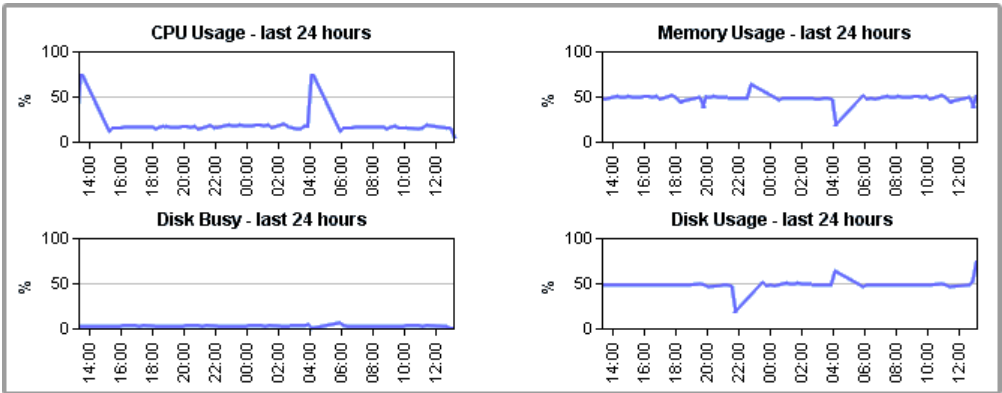
- **CPU Usage:** the percentage of the system's CPU resources that are being used
- **Memory Usage:** the amount of memory, expressed as a percentage of total available memory, being consumed by a process
- **Disk Busy:** the percentage of time that the disk is handling transactions in progress
- **Disk Capacity:** the percentage of space on the system disk that is being used

The thresholds for the service status indicators are typically 70% for a warning state, and 90% for a critical state. These thresholds can be customized (see [Changing Reporting Thresholds](#)).

Note that if data are not yet available (e.g., the Element in focus is newly added), the gauges will report as unavailable until a time interval has passed; if there are data, but no recent data (e.g., an Element is no longer down), there will be minimum and maximum dials, but no main average dial until a sample of data has been collected.

24-Hour Performance Graphs

While the gauges each display a minimum, maximum, and average value; the full 24-hour performance history is displayed in the graphs below:



Element Tables

All server-type Elements and Element Groups that make up your monitored inventory are displayed below the graphs

Elements						
	Name	CPU Usage	Memory Usage	Disk Busy	Disk Capacity	Network - In / Out
	AIX DEV LPAR (dev1-lpar-aix33)	1%	23%	1%	23%	34 pbits/s / 32 pbits/s
	Bamboo (build-bamboo)	2%	73%	0%	67%	20 kbits/s / 1 kbits/s
	exch-ad02 (exch-ad02.rdl.local)	2%	95%	0%	28%	24 kbits/s / 127 kbits/s
	McKay (mckay)	0%	27%	0%	91%	0 kbits/s / 0 kbits/s
	Novell (lab-novell65)	1%	82%	0%	0%	0 pbits/s / 0 pbits/s
	Opteron (opteron)	1%	75%	0%	66%	18 kbits/s / 9 kbits/s
	SnoopRdog (snoopy)	13%	95%	0%	64%	0 kbits/s / 0 kbits/s
	The Zones A (vmb-t1k-a)	2%	76%	1%	27%	34 kbits/s / 19 kbits/s
	VMI RD6 (vmb-rd6)	22%	7%	0%	25%	443 pbits/s / 1739 pbits/s
	VMI RD7 (vmb-rd7)	28%	6%	0%	46%	587 pbits/s / 566 pbits/s
Groups						
	Name	CPU Usage	Memory Usage	Disk Busy	Disk Capacity	Network - In / Out
	Quality Assurance	2%	28%	0%	25%	34.7 / 37.3

The following information is displayed in sortable columns:

- CPU Usage: the percentage of CPU resources that are being used
- Memory Usage: the amount of memory, expressed as a percentage of total available memory, that is being consumed by a process
- Disk Busy: the percentage of time the disk is handling transactions
- Disk Capacity: the percentage of storage space on the system disk that is being used
- Network In: the average amount of traffic coming in over the network interface
- Network Out: the average amount of traffic going out over the network interface

In this section of the dashboard, the servers are presented as they have been organized in **My Infrastructure**. If applicable, you can click top-level Groups to display the group's servers and (if applicable) subgroups. As you click group or server names, the status reported in the gauges and charts reflects your current location in your infrastructure, whether it is parent groups, nested groups, or individual servers.

When viewing a group, you can navigate to other groups by selecting the name of the group from the **Current Location** dropdown list at the top of the dashboard:

Current Location: My Enterprise -> Email Systems

## Viewing All SLAs

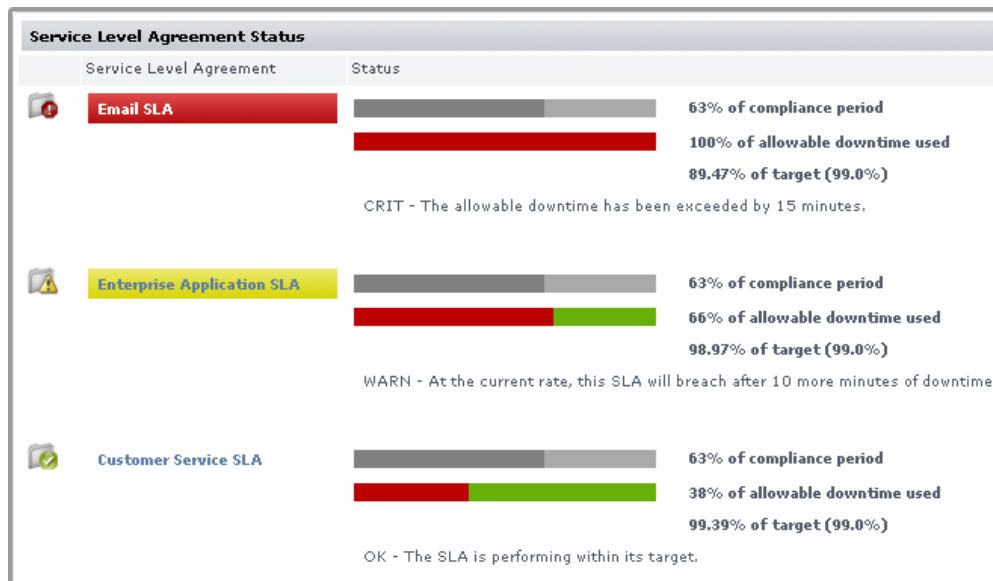
Service level agreements on the **SLAs** dashboard indicate whether performance targets are being met. Although the main summary displays the status of the SLA definition as a whole, you can also expand the view to verify how well component service level objectives (SLOs) are meeting targets. (SLOs are made up of monitored services that, as a group, are used to measure a specific performance goal.)

In the **Service Level Agreements** subpanel (accessed by clicking the **SLAs** tab), the following SLA information is provided in the default view:



- the list of SLAs, and whether any are in a critical or warning-level state
- headway into the time period during which compliance is measured
- the percentage of allowable downtime used, after which the SLA's status becomes critical

## SLA Status Indicators

The color coding used in the **Service Level Agreements** subpanel indicates, at a glance, whether the SLAs' respective limits are in danger of or have already been exceeded:



The **Downtime** progress bar allows you to gauge how close the SLA is to reaching a critical state:

- an SLA whose allowable downtime exceeds 100% reaches a critical state, is highlighted with red, and is accompanied by the critical state icon ()
- an SLA whose allowable downtime, at the current rate of use, will be depleted before the compliance period has ended enters a warning-level state, is highlighted with yellow, and is accompanied by the warning state icon ()
- an SLA whose graphed allowable downtime does not exceed the graphed progress through the compliance period is in a compliant state

Note that once an SLA reaches a critical state, it will remain in that state until the compliance period has restarted the following week or month; an SLA that enters a warning-level state can be downgraded to a normal state if the rate at which allowable downtime is used decreases to a "safer" value.

## Generating an SLA Detailed Report

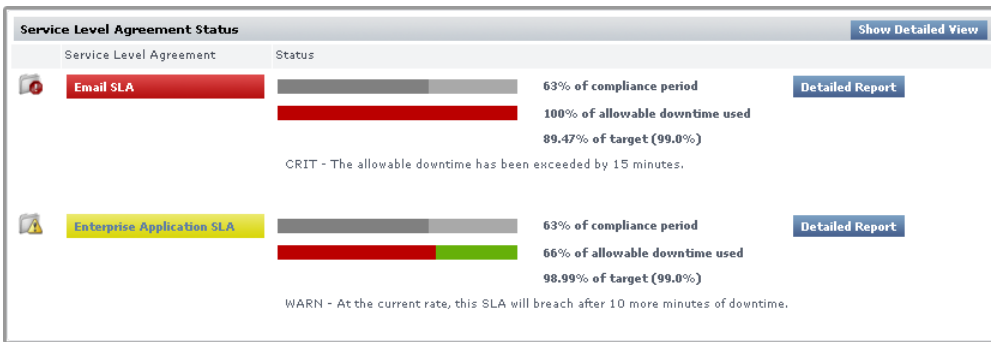
Clicking an SLA's corresponding **Detailed Report** button instantly generates an SLA Detailed report for the last 24 hours.

See [Reports for Service Level Agreements](#) for more information.

## SLA View Types

The **Service Level Agreements** subpanel provides two types of views: Condensed View and Detailed View. The latter view is suitable if you have one or two defined SLAs.

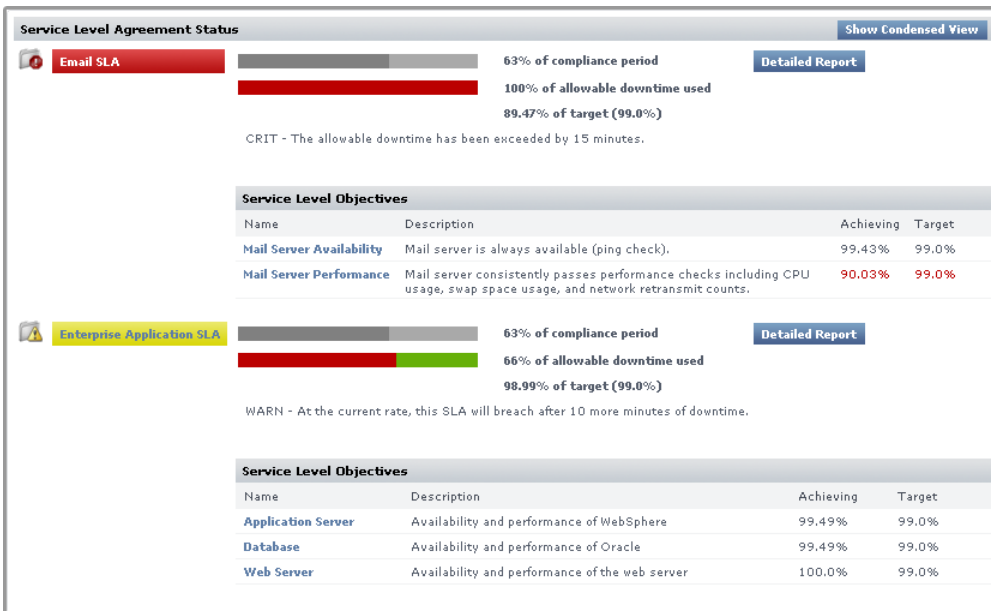
Condensed View



The Condensed View is the default view of this subpanel and displays the following information:

- the name of the SLA
- a status breakdown of the SLA for the current time period:
- time period elapsed
- available downtime used for the current time period
- how close the SLA is to its performance target
- status message

Detailed View



Click the **Show Detailed View** button to expand each SLA to include SLOs.

An SLA's compliance is based on the downtime of its component SLOs: when one or more of the SLOs experience downtime, it counts towards overall SLA non-compliance.

Clicking an SLO name displays the status of the SLO, and all of the services that make up the SLO:

Service Level Objective			
Name	WebSphere		
Description			
Monitoring Period	Every Mon,Tue,Wed,Thu,Fri 9:00AM-6:00PM		
Compliance Period Type	Weekly		
Target Percentage	99.0		
Member Service Monitors			
Name	Element	Status	Description
WebSphere	WebSphere (lab-websphere51)	CRIT	
Plants Response	WebSphere (lab-websphere51)	CRIT	
File System Capacity	WebSphere (lab-websphere51)	CRIT	
PING-lab-websphere51	WebSphere (lab-websphere51)	OK	Default ping check for lab-websphere51

Using the Detailed View allows you to pinpoint which SLO is causing SLA non-compliance, and in turn which monitors are causing the SLO to experience downtime.

For more information about viewing SLA details, and defining SLOs that help you accurately gauge the performance of your IT infrastructure, see [Working with Service Level Agreements](#).

## Viewing All Applications

Applications provide the overall status for one or more services that up.time monitors. Applications group services, such as ping checks and checks for the status of the up.time agents that are installed on a system. An Application can contain many services, and enable you to better analyze component outages versus true Application outages.


An Application consists of:

- master service monitors: one or more monitors can be used to determine the status of the Application as a whole
- regular service monitors: other service monitors that are associated with a master service monitor, but are not used to determine the status of the Application as a whole

The status of each Application is color coded:

- Applications highlighted in green are functioning normally
- Applications highlighted in yellow are in a warning state







The color coding also indicates whether an Application is offline or is in scheduled maintenance:

- an Application that is offline is highlighted in red and marked by the offline icon, and a message indicating that the Application is offline appears in the **Applications** subpanel
- an Application that is in scheduled maintenance is grayed out, the message *System is in scheduled maintenance* is displayed in the **Applications** subpanel, and the Application is marked with the scheduled maintenance icon (  )

The **Applications** subpanel displays the status of each Application that you have added to up.time.

This subpanel has two views: [Condensed View](#) and [Detailed View](#).

## Condensed View

Application Status			Show Detailed View
Application Name	Description	Status of Master Services	Status of Regular Services
 AIX	--		
 Enterprise App	--		
 Mail Servers	--		
 Databases	--		

The Condensed view is the default view for this subpanel and displays the following information:

- the name of the Application
- a description of the Application, if one was added when the Application was defined
- the status of each service in the Application

The status of the service is denoted by a colored bar in the **Status of Master Services** and **Status of Regular Services** columns. For example, if there are three services associated with the Application and their status is OK then three green bars appear in this column.

## Detailed View

Application Status				Show Condensed View
Application Name	Description	Element	Monitor Information	
<b>AIX</b>	--			
* FSCap (member)	--	AIX QA LPAR	/usr is 53% full	
* FSCap (member)	--	AIX DEV LPAR	/is 97% full	
* FSCap (member)	--	AIX5	/var is 100% full, /usr is 92% full, / is 90% full, /opt is 88% full	
* PING-10.1.1.56	Default ping check for 10.1.1.56	AIX QA LPAR	Ping completed: 1 sent, 0.0% loss, 1.0ms average round trip time	
* PING-10.1.1.57	Default ping check for 10.1.1.57	AIX DEV LPAR	Ping completed: 1 sent, 0.0% loss, 0.0ms average round trip time	
* PING-aix5l	Default ping check for aix5l	AIX5	Ping completed: 1 sent, 0.0% loss, 1.0ms average round trip time	
Application Name	Description	Element	Monitor Information	
<b>Enterprise App</b>	--			
* Oracle Advanced	--	HP Integ	All requested values queried successfully	
* PING-10.1.1.232	Default ping check for 10.1.1.232	lab-t1-2	Ping completed: 1 sent, 0.0% loss, 1.0ms average round trip time	
* ping-test	Default ping check for hointeg	HP Integ	Ping completed: 1 sent, 0.0% loss, 0.0ms	

Click the **Show Detailed View** button to change to the Detailed view of the **View Applications** subpanel.

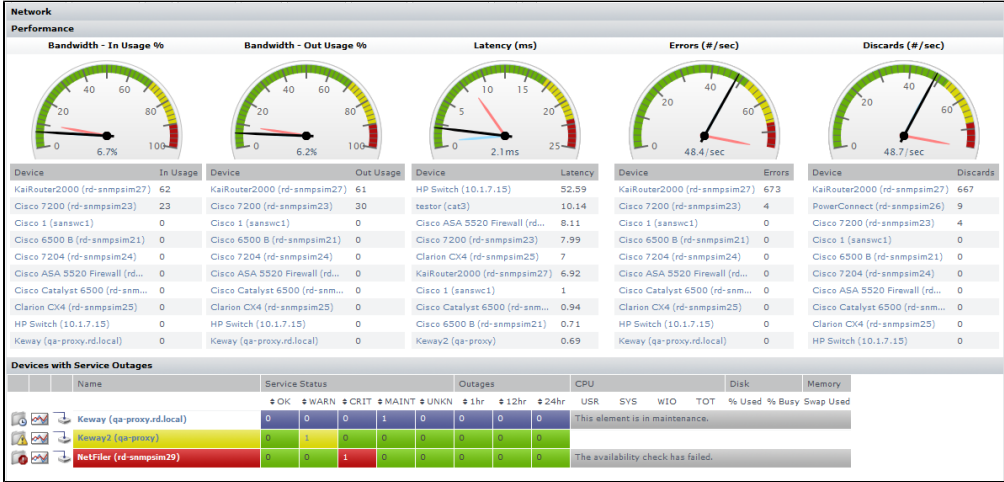
The name of the master Application group is listed (**AIX** in the image above) along with the names of the individual service monitors (e.g., **FSCap**). Master service monitors in an Application are marked with an asterisk (\*).

The status of a service is denoted by a colored bar beside the name of the service: green indicates the service is functioning normally; yellow means the service is in a warning state; and red indicates the service is in a critical state.

The name of each Application is a hyperlink. Click a link to view detailed information about an Application.

## Viewing the Network Dashboard

The network dashboard is a summary of network device performance, and network-based service monitor outages. It is automatically updated every 30 seconds. You can view this dashboard by clicking the **Network** tab.



The network dashboard provides you with a single view of your network environment, and keeps you abreast of any network-related issues:

- instantly spot network capacity issues, and compare trends over the past day
- pinpoint top resource consumers to help resolve performance bottlenecks before they cause an outage
- immediately spot network devices that are currently failing, and click through to investigate the root cause

The following metrics are together used to report network performance:


In Usage	global inbound bandwidth usage of all monitored network devices' ports
Out Usage	global outbound bandwidth usage of all monitored network devices' ports
Latency	network device latency values collected through each monitored Element's ping monitor does not include network devices without an assigned ping monitor
Errors	the average number of errors per second through all monitored network device ports
Discards	the average number of packets discarded per second through all monitored network device ports

For each category, there is a performance gauge that displays the average for all monitored ports based on the most recent sample. Maximum and minimum values over the last 24 hours is also shown. Note that the first two metrics are percentage-based, and their gauges are static; the remaining three metrics' gauges may scale if the recorded value exceeds the default upper limit. The thresholds for the service status indicators are typically 70% for a warning state, and 90% for a critical state.

Additionally for each category, there are top-10 lists displaying the individual Elements that are using the most bandwidth, have the highest latency, or seeing the most errors or discarded packets. Clicking any Element name will display its Quick Snapshot page, where you can further investigate bottlenecks.
































Devices with Service Outages

Any network device Element whose attached service monitors are experiencing outages are displayed in this section. For convenience, you can sort the results by number of current outages, or outage occurrences.

 If the dashboard is being viewed by an up.time user who does not have permission to view all Elements, and as a result, may not be able to see network device Elements, the list will be empty, and up.time will report that there are not any available network devices.

Viewing All Elements

Elements are the systems, network devices, Applications, and SLAs that up.time is currently monitoring. You can view the status of all monitored Elements on the **All Elements** dashboard. This can be accessed by clicking the **All Elements** tab.

All Elements																
	Name	Service Status					Outages			CPU				Disk		Memory
		OK	WARN	CRIT	MAINT	UNKN	1hr	12hr	24hr	USR	SYS	WIO	TOT	% Used	% Busy	
	AIX DEV LPAR (dev1-lpar-aix53)	2	0	0	0	0	0	0	0	0%	1%	0%	1%	76%	0%	1%
	Bamboo (build-bamboo)	2	0	0	0	0	0	0	0	9%	1%	0%	10%	81%	1%	54%
	logus	0	0	0	0	0	0	0	0	This element is in maintenance.						
	ench-ad02 (ench-ad02.rd1.local)	1	0	1	0	0	1	0	0	1%	0%	0%	1%	20%	2%	92%
	Google (www.google.ca)	0	0	0	0	0	0	0	0	0%	0%	0%	0%	0%	0%	0%
	HMC Managed Server (lab1-p9110)	0	0	0	0	0	0	2	0							
	McKay (mckay)	2	0	0	0	0	0	0	0	0%	0%	0%	0%	98%	0%	0%
	Novell (lab-novell65)	1	0	0	0	0	0	0	0	n/a	n/a	n/a	0%	0%	n/a	52%
	Opteron (opteron)	2	0	0	0	0	1	0	0	No recent performance data available. Is the system online?						
	Perl (ntp.perl.org)	0	0	0	0	0	0	0	0							
	QA Active Directory 01 (qa-ad01)	0	0	1	0	1	1	1	0	The availability check has failed.						
	QA Active Directory 02 (qa-ad02)	1	1	0	0	0	0	0	0	94%	4%	0%	96%	60%	4%	23%
	QA Appserver Three (qa-appserver3)	2	0	0	0	0	0	0	0	1%	1%	4%	6%	100%	0%	1%
	QA Exchange Server (qa-exchange01)	2	0	0	0	0	0	0	0	2%	0%	0%	2%	51%	0%	62%
	QA Splunk (qa-splunk)	2	0	0	0	0	0	0	0	0%	0%	0%	0%	48%	0%	1%
	qa-agent00.rd.local (qa-agent00)	2	0	0	0	0	0	0	0	1%	3%	0%	4%	22%	0%	0%
	qa-agent01.rd.local (qa-agent01)	2	0	0	0	0	0	0	0	0%	0%	0%	0%	33%	0%	0%
	qa-agent02.rd.local (qa-agent02)	2	0	0	0	0	0	0	0	0%	0%	0%	0%	23%	0%	0%
	qa-agent03.rd.local (qa-agent03)	2	0	0	0	0	0	0	0	0%	0%	0%	0%	23%	0%	0%
	qa-agent04.rd.local (qa-agent04)	2	0	0	0	0	0	0	0	0%	0%	0%	0%	54%	0%	0%
	qa-agent05.rd.local (qa-agent05)	2	0	0	0	0	0	0	0	0%	1%	0%	1%	23%	0%	0%
	qa-ain61	2	0	0	0	0	0	0	0	0%	1%	0%	1%	100%	0%	1%
	qa-esch2010 (qa-esch2010.rd1.local)	0	0	0	2	0	0	0	0	This element is in maintenance.						
	qa-ora11-rhe52	2	0	0	0	0	0	0	0	20%	4%	0%	24%	62%	2%	0%
	qa-ora112-rhe54	2	0	0	0	0	0	0	0	1%	1%	1%	3%	76%	0%	11%
	qa-rhe55-ut4	2	0	0	0	0	0	0	0	1%	3%	0%	4%	38%	1%	1%
	qa-sql2k5-w2k3	2	0	0	0	0	0	0	0	0%	0%	0%	0%	16%	0%	1%
	qa-sql2k8-w2k8	2	0	0	0	0	0	0	0	0%	0%	0%	0%	53%	0%	0%
	qa-sql2k8r2-00	2	0	0	0	0	0	0	0	3%	2%	0%	5%	59%	1%	28%
	qa-tools	2	0	0	0	0	0	0	0	1%	1%	1%	3%	46%	17%	0%
	qa-w2k3-auto00	2	0	0	0	0	0	0	0	0%	0%	0%	0%	65%	0%	1%

The **Elements** subpanel lists the following information:

- the names of the Elements in your environment
- the status of the services that are assigned to each Element
- the number of outages over the last hour, 12 hours, and 24 hours
- the percentage of CPU resources being consumed by users, the system, and by disk I/O
- the percentage of the system disk that is being used and the percentage that is busy
- the amount of memory swap space that is being used

For convenience, you can sort the Elements table by any outage type.

If up.time cannot contact an Element, the reason will be displayed:

- The availability check has failed.
- This element is in maintenance.
- This VM is currently powered off.

The values in each column are hyperlinks. Click one of the links to display the following information in the system information or graphing subpanels:

- Click any value in the **OK**, **WARN**, **CRIT**, **MAINT**, or **UNKNOWN** columns to open the Element's **Status** subpanel.
- Click any value in the **Outages** column to open the Element's **Outages** subpanel.
- Click any value in the **USR**, **SYS**, **WIO**, or **TOT** columns to open the Element's **Usage% Busy** report subpanel. For more information, see [Usage \(% busy\)](#) for more information.



- Click any value in the **% Used** column to open the Element's **File System Capacity** report subpanel. See [File System Capacity Graph](#) for more information.
- Click any value in the **% Busy** column to open the Element's **Disk Performance Statistics** report subpanel. See [Disk Performance Statistics Graph](#) for more information.

**i** By default, Elements in **WARN** or **CRIT** states, in maintenance, or whose status is undetermined are displayed. To display all Elements regardless of status, unselect the **Hide OK Elements** check box.

## Viewing All Services

Services are specific tasks, or sets of tasks, performed by an application in the up.time environment. up.time service monitors continually check the condition of services to ensure that they are providing the required functions to support your business. For more information on services, see [Understanding Services](#).

You can view the services assigned to each system in your environment by clicking on the **All Services** tab. This tab contains the following information in sortable columns:

- the name of the service
- the Element that is associated with the service
- the status of the service
- whether an outage has been acknowledged
- the date and time on which the last check was performed
- the number of days, hours, and minutes since the last check
- a human-readable text message that was returned by the monitor (e.g., up.time agent running on MailServer, up.time agent 3.7.2 linux)

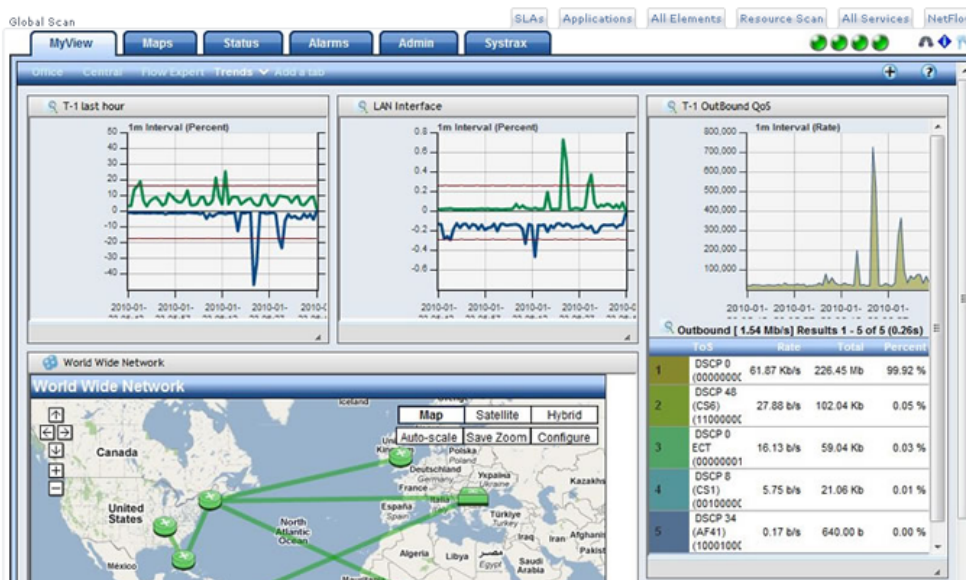
**i** By default, services in **WARN** or **CRIT** states, or services whose associated Element is in maintenance or an undetermined state are displayed. To display all services regardless of status, unselect the **Hide OK Service Monitors** check box.

## Viewing Scrutinizer Status

Scrutinizer is a NetFlow analyzer that takes advantage of communications standards for Cisco IOS networking devices, and other compatible switches and routers, to retrieve and store network traffic information for users, systems, and applications. It allows administrators to monitor, graph, and report on network usage patterns, and locate the heaviest traffic creators.

Scrutinizer can be integrated with up.time. Doing so allows you to add network devices that are exporting NetFlow data to Scrutinizer, as well as call a Scrutinizer instance, from a commonly-monitored Element's status page (whether the Element is a NetFlow-exporting network device, or another type of up.time Element).

You can also access all of Scrutinizer's features, such as the **MyView** status panel, from the **Dashboards** tab by clicking the **NetFlow** tab:



## Changing Reporting Thresholds

The thresholds that determine when an Element's reported status changes between normal, Warning, and Critical (i.e., green, yellow, and red) can be modified for both the **Global Scan** and the **Resource Scan** dashboards.



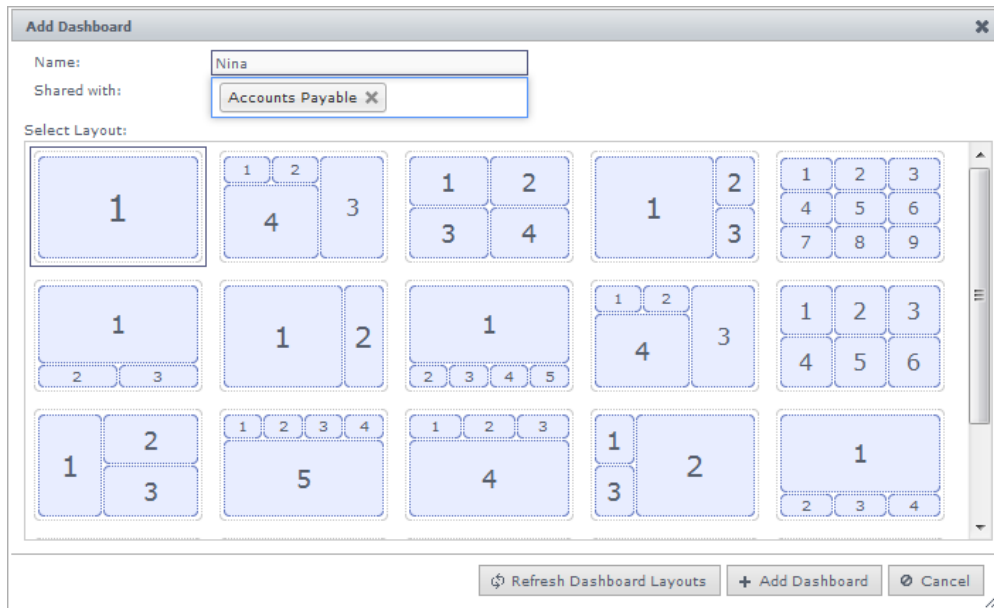
**Global Scan** and **Resource Scan** thresholds are configured by separate sets of attributes that can be changed in the **up.time Configuration** panel. By changing these attributes, you can set how large the color ranges are on resource gauges, and at what point table cells change color. See [Status Thresholds](#) for more information.

Note that when you change **Global Scan** threshold values, the changes are not retroactively applied to all existing Elements monitored by up.time; changes only apply to Elements added to up.time after the threshold changes are made. Conversely, the **Resource Scan** gauge ranges are updated immediately.

## Custom Dashboards

User-created dashboards allow your various up.time users to create views that augment or replace the default dashboards. While dashboards are still created to display historical data or current Element status, they are tailored to specific users or user groups. A custom dashboard can be designed to augment the default dashboards, or in some cases, replace them altogether.

Dashboards are based on one of various layouts, then completed by configuring component gadgets:



Gadgets, after being developed, interface with up.time using the up.time Controller. Refer to the [Integration Guide](#) for more information.

Dashboards can be created by any up.time user, and shared with the user group they belong to.

## Adding Dashboards

1. On the main **Dashboards** tab, click either the Add subtab, or click the configuration icon on the far right of the tab row. A layout browser appears, showing various customization choices.
2. **Name** the dashboard.  
The dashboard name is used on the dashboard tab. There is a 24-character limit.
3. Configure whether this dashboard will be **Shared with** other user groups by clicking in the field, then selecting groups. You can only share your dashboard with groups that you are a member of, unless you are an up.time administrator with the `superadmin` user role.
4. Click to select a dashboard layout.
5. Click **Add Dashboard**.  
You will be presented with an empty dashboard, with a wireframe layout.
6. Click an empty slot to add a gadget.  
The **Add Gadget** browser is displayed.
7. Configure and add the gadget depending on its properties.  
Configuration may include giving the dashboard a name that will act as its title in the dashboard layout.
8. Continue to add and configure gadgets until the dashboard is complete.

## Managing Dashboards

Although dashboards are easily shared among user group members, there are management rules:

- only the dashboard creator can change its name and share permissions, or delete the dashboard
- sharing a dashboard means everyone in the user group can also see the dashboard, but none of them can make changes to it
- administrators with the `superadmin` role can see all user-created dashboards, but cannot change them

It is possible to make a custom or default dashboard a "primary" view:

- every dashboard can be rendered as a fullscreen view

- any dashboard can be set as the landing page for each user account (see [Adding Users](#) for more information)



If your up.time deployment includes a UI instance, in order for dashboards to be shared and viewed across both instances, the UI instance needs to be able to access the auxiliary gadget files on the core Monitoring Station. See [User Interface Instance Settings](#) for more information.

## Sample Custom Dashboards

In addition to the standard dashboards, there are two custom dashboard examples that showcase some of the gadgets that are included with up.time:

- **Custom Example:** uses one of the multi-cell layouts to present the different bundled gadgets that indicate element status:
  - Group Status Chart
  - Element Status Chart
  - Incident Panel
  - Topology Tree
- **Map:** demonstrates how you can use the Pin on Image gadget to visually arrange your servers on a geographical map

For information about each gadget, see [Dashboard Gadgets](#).